REMARKS

These remarks are responsive to the Office Action mailed December 8, 2006.

Independent claims 1 and 29

Claims 1-8 and 29-33 are rejected under 35 U.S.C. §103(a) as being unpatentable over Brown et al. et al. in view of Hwangbo and further in view of Fischer. Reconsideration and withdrawal of these rejections are respectfully requested.

Claim 1 recites:

> **the authority of the user defined within the second code portion of the certificate being verifiable by the server computer independently of the digital certificate by accessing, over the network, a store of authority information that is independent of the digital certificate and by matching the authority of the user defined within the second code portion of the certificate to corresponding authority information of the user retrieved from the accessed independent store of authority information.**

Claim 29 recites:

> **code for accessing, over the network, a store of authority information that is independent of the digital certificate and that stores corresponding authority information, the accessing code being configured to match the authority of the user defined within the second code portion of the certificate to the corresponding authority information accessed from the independent store to validate the rights of the user to data and programs within the computing environment.**

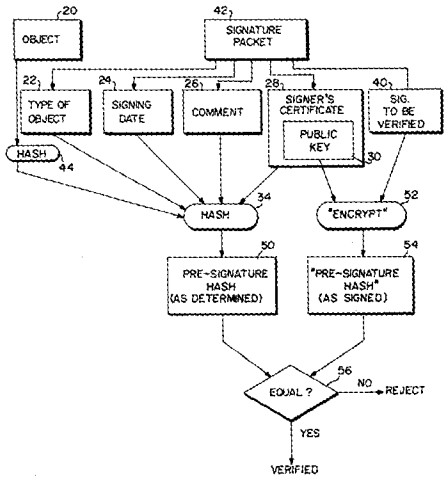
Therefore, each claim recites that the authority of the user defined in the second code portion of the certificate is verifiable independent of the digital certificate. This is done, according to the claims, by accessing a store of authority information that is independent of the digital certificate and matching the authority information accessed from the independent store with the authority information defined within the digital certificate. If they match, the authority defined in the second portion of the digital certificate is verified (claim 1) or the rights of the user to data and programs within the computing environment defined within the second portion of the digital certificate are validated (claim 29).

It is respectfully submitted that both claims recite that the authority defined within the certificate is verifiable (or may be validated) by accessing a store of information that is independent of the digital certificate.

It is acknowledged that the primary combination to Brown et al. and Hwangbo do not teach or suggest such subject matter – hence the addition of Fischer to the applied combination. Indeed, for an alleged teaching of the subject matter acknowledged to be missing in Brown et al. and Hwangbo, the Office relies on Fischer.

The Office points to claim 1 and Fig. 3 (reproduced below) of Fischer for this teaching.

FIG. 3



As is apparent, Fig. 3 shows a method of verifying a digital signature. In fact, the brief description of Fig. 3 states:

> **FIG. 3 is a flow diagram that indicates how a digital signature created in accordance with FIG. 2 is verified;**

Fig. 3 does not teach or suggest (whether considered alone or in combination with Brown et al.-Hwangbo) verifying the authority defined within a digital certificate.

The detailed description of Fig. 3 states that to verify the signature, a presignature hash 50 is generated by the recipient of the transmitted message (col. 16, lines 28-35). The recipient

then uses the public encryption key of the transmitted certificate 28 and performs an encrypt operation 52 … to generate a presignature hash 54 (col. 16, lines 36-40). The values of the two presignature hashes 50 and 54 are then compared and the received signature is rejected as being invalid unless the two quantities 50 and 54 match (col. 16, lines 44-46).

However, the description continues stating that other steps are then carried out to insure that the person has the authority stipulated in the certificate (col. 16, line 56):

> another signature or a certificate. To complete the validation process, the recipient analyzes the certificates associated with the signature to determine that the proper authority has been conveyed to each certificate through its signatures and the antecedent certificate(s) of these authorizing signatures.

Therefore, Fischer teaches that to verify the "authority" defined by a certificate, you verify that proper "authority" has been conveyed to each certificate through its signatures and the antecedent certificates of these authorizing signatures. The word "authority" is placed between quotation marks, because the word in Fischer does not have the same meaning as the same word in the present claims. Indeed, as noted in the above passage, "authority" in Fischer means the validity of the certificate holder – meaning, whether the certificate has been issued from some person or entity having the authority to issue such a certificate. In the present claims, however, the authority defined is the authority of a "user … to request that the server computer carry out a requested action" (claims 1, 29) or "the authority of the user defined within the second code portion of the certificate defining access rights of the user to data and programs within the computing environment" (claim 29).

Col. 10, line 66 to col. 11, line 10 explains what is meant by "antecedent certificates" in the previous passage:

> To be valid a certificate must be signed by the private key(s) associated with one or more other valid certificates which are hereafter referred to as antecedents to

> that certificate. These may also be accompanied by restrictions and/or mandatory restraints which must be met (such as, perhaps, co-signatures). Each of these antecedent certificates must grant the signer the authority to create such a signature and/or to issue the purchase order in our example. These may also be accompanied by restrictions and/or mandatory restraints which must be met (such as, perhaps, co-signatures). Each of the antecedent certificates may in turn have its own antecedent(s).

Therefore, to verify "authority" (i.e., whether the certificate was properly issued by an entity having the authority to do so), Fischer teaches to examine the signatures of any and all certificates in the chain of certificates that terminates at the certificate whose "authority" is under examination. These certificates in the chain of certificates are Fischer's "antecedent certificates." Fischer, in effect, teaches to verify the signatures of all certificates in the chain of certificates, all the way up to the authority of the CA (Certificate Issuing Authority). In fact, Fischer teaches that it is the sender's responsibility to make this verification possible by sending all generations of antecedent certificates to the recipient to make sure that the recipient can, indeed, verify this chain of "authority" tied to the antecedent certificates (col. 21, lines 43-47):

> ject. The sender of the object (e.g., the purchase order) has the responsibility of sending all generations of antecedent certificates and signatures (up to and including the meta-certificate) which are needed for a recipient to perform validation operations.

As should be clear now, Fischer does not teach or suggest (whether considered alone or in combination with Brown et al.-Hwangbo), that the authority defined within a digital certificate is verifiable by accessing a store of information that is independent of the digital certificate, as claimed. At the outset, the authority in the claims is the authority of the certificate holder to request that the server "carry out a requested action", which is not even addressed in Fischer or the Brown et al.-Hwangbo-Fischer combination. Moreover, to verify what Fischer calls "authority" (determining whether a received certificate was validly issued by examining its signatures, co-signatures and counter-signatures), Fischer calls for the recipient to examine not

only the received certificate but to also all antecedent certificates, that is, the chain of certificates that ultimately resulted in the received certificates (the received certificate's parents and ancestors, as it were). Such is not a store of authority information that is independent of the digital certificate, as required by the claims. Quite to the contrary, a certificate's antecedent certificates are not, by definition, "independent of the digital certificate" – they are intimately connected to the digital certificate being validated – in fact, they are the predecessor certificates and are so inextricably linked to one another that each higher member of the chain is the parent of the lower member of the chain. The group of antecedent certificates is not, therefore, "a store of authority information that is independent of the digital certificate", as required by both claims 1 and 29, whether the teachings of Fischer are considered alone or collectively with those of Brown et al. and Hwangbo, whose shortcomings necessitated the inclusion of Fischer in the applied combination of the present Office Action.

Reconsideration and withdrawal of the 35 USC §103(a) rejections of claims 1 and 29 and their respective dependent claims are, therefore, respectfully requested.

Independent Claims 9 and 15

Claims 9-13 and 15-19 are rejected under 35 U.S.C. §103(a) as being unpatentable over Brown et al. in view of Fischer. Reconsideration and withdrawal of these rejections are respectfully requested.

Claim 9 recites:

> **validating the authority information included within the received certificate by accessing a store of authority information that is coupled to the network and that is independent of the received certificate and by matching the authority information included within the received certificate to authority information that is associated with the user and that is stored in the accessed independent store of authority information, and**

Claim 15 recites:

> **authorization validating code configured to enable validation of the authority information within the received certificate against corresponding authority information for the user stored in a data structure that is coupled to the network and that is independent of the received certificate by accessing the data structure over the network and by matching the authority information included in the received certificate to the corresponding authority information stored in the accessed data structure.**

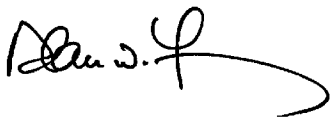
As with claims 1 and 29, independent claims 9 and 15 require that the verification/validation of the authority information within the received certificate be carried out against corresponding authority information accessed from a store of authority information that is independent of the received certificate. As such, the above arguments are equally applicable here. Rather than repeating them nearly *verbatim*, they are simply incorporated herein by reference, as if repeated in full.

In short, the Brown et al.-Fischer combination does not teach or suggest to verify the authority of the certificate holder (as opposed to the validity of the certificate, as in Fischer) by accessing a store of authority information that is independent of the received certificate. Again, Fischer verifies the "authority" by examining the received certificate's ~~pedigree~~ antecedent certificates (which must be sent to the recipient along with the current certificate (col. 21, lines 43-48). According to the claimed embodiments, the verification of the authority of the certificate holder is an authority to do something: a) to make a payment request (claim 9); or b) to carry out a financial transaction (claim 15), which is not something that may be verified by examining the digital signatures of previous generations of certificates that resulted in the received certificate. Moreover, Fischer's previous generations of certificates cannot be said to be independent of the received certificate. Quite the contrary, Fischer's antecedent certificates are inextricably bound to the received certificate, and in no way independent thereof, as required by claims 9 and 15. Therefore, Fischer, whether considered singly or in combination with Brown et al. (which has

previously been shown, to the satisfaction of the Office, not to anticipate the claims), does not teach or suggest the claimed subject matter. Reconsideration and withdrawal of the rejections of claims 9 and 15 and that of their respective dependent claims are, therefore, respectfully requested.

Applicants believe that this application is now in condition for allowance. If any unresolved issues remain, please contact the undersigned attorney of record at the telephone number indicated below and whatever is necessary to resolve such issues will be done at once.

Respectfully submitted,



Date: February 25, 2007 By:_____

Alan W. Young
Attorney for Applicant
Registration No. 37,970

YOUNG LAW FIRM, P.C.
4370 Alpine Rd., Ste. 106
Portola Valley, CA 94028
Tel.: (650) 851-7210
Fax: (650) 851-7232

\\Ylfserver\ylf\CLIENTS\ORCL\5881 (OID-2003-142-01)\5881 AMEND.3.doc